Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, therefore the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
  - BFCommand & Control Server Managers Multiple Vulnerabilities
  - Home FTP Server Arbitrary File Access
  - LeapFTP Arbitrary Code Execution
  - IMRadio Password Disclosure
  - Microsoft Internet Explorer Arbitrary Code Execution
  - Symantec AntiVirus Corporate Edition and Client Security Privilege Elevation
  - BlueWhaleCRM SQL Injection
  - ZipTorrent Password Disclosure
- UNIX / Linux Operating Systems
  - **Alexis Sukrieh Backup Manager Information Disclosure (Updated**
  - Astaro Security Linux HTTP CONNECT Unauthorized Access**)**
  - **BlueZ Arbitrary Command Execution (Updated)**
  - **Bzip2 Remote Denial of Service (Updated)**
  - **Courier Mail Server Remote Denial of Service (Updated)**
  - **Elm 'Expires' Header Remote Buffer Overflow (Updated)**
  - **FreeRadius 'rlm_sql.c' SQL Injection & Buffer Overflow (Updated)**
  - **GNU shtool Insecure Temporary File Creation (Updated)**
  - HP-UX Veritas File System Information Disclosure
  - Inter7 SqWebMail HTML Email Arbitrary Code Execution
  - **LM_sensors PWMConfig Insecure Temporary File Creation (Updated)**
  - Maildrop Lockmail Privilege Elevation
  - **Kismet Multiple Remote Vulnerabilities (Updated)**
  - MPlayer Audio Header Buffer Overflow
  - **Multiple Vendors TLS Plaintext Password (Updated)**
  - **LBL TCPDump Remote Denials of Service (Updated)**
  - **Multiple Vendors Zlib Compression Library Buffer Overflow (Updated)**
  - **Multiple Vendor dhcpcd Denial of Service (Updated)**
  - Multiple Vendors Linux Kernel 64 Bit ELF Header Denial of Service
  - **Multiple Vendors Linux Kernel IPSec Policies Authorization Bypass (Updated)**
  - Multiple Vendors Simpleproxy HTTP Proxy Reply Format String
  - **Multiple Vendors Kerberos V5 Multiple Vulnerabilities (Updated)**
  - **Multiple Vendors GNOME Evolution Multiple Format String (Updated)**
  - **Multiple Vendors LibXPM Bitmap_unit Integer Overflow (Updated)**
  - Nokia Affix BTSRV Device Name Remote Command Execution
  - PADL Software PAM_LDAP Authentication Bypass
  - **PCRE Regular Expression Heap Overflow (Updated)**
  - PAFileDB 'Auth.PHP' SQL Injection
  - PHPMyAdmin Cross-Site Scripting
  - RedHat XNTPD Insecure Privileges
  - slocate Long Path Denial of Service
  - **Sun ONE/iPlanet Messaging Server Arbitrary Code Execution (Updated)**
  - Sun Solaris DHCP Client Remote Code Execution
  - Tor Weak Diffie-Hellman Handshake
  - UMN Gopher Client Remote Buffer Overflow
- Multiple Operating Systems
  - Alexander Palmo Simple PHP Blog Directory Traversal
  - Alexander Palmo Simple PHP Blog Remote Arbitrary File Upload
  - All Enthusiast, Inc. PhotoPost Cross-Site Scripting
  - CVS 'Cvsbug.In' Script Insecure Temporary File Creation
  - Looking Glass Input Validation
  - e107 Forum_post.PHP Non-existing Forums
  - Flagship Industries Ventrilo Status Requests Remote Denial of Service
  - Foojan PHPWeblog Cross-Site Scripting
  - FreeStyle Wiki Arbitrary Perl Command Execution
  - Gallery Cross-Site Scripting
  - Helpdesk Software Hesk Authentication Bypass
  - HP OpenView Network Node Manager Remote Arbitrary Code Execution
  - **FUDForum Security Restriction Bypass (Updated)**
  - FUDforum Avatar Upload Arbitrary Script Upload
  - **InterSpire ArticleLive NewComment Cross-Site Scripting (Updated)**
  - Jelsoft Enterprises vBulletin 'backup.php' Information Disclosure

- Lithium Software Quake 2 Lithium II Mod Format String
- **Mozilla Firefox Multiple Vulnerabilities (Updated)**
- Multiple Vendors Apache Remote Denial of Service
- **Multiple Vendors PHPXMLRPC and PEAR XML_RPC Remote Arbitrary Code Execution (Updated)**
- **Multiple Vendors XML-RPC for PHP Remote Code Injection (Updated)**
- MyBB SQL Injection
- **MySQL 'mysql_install_db' Insecure Temporary File Creation (Updated)**
- PHP-Fusion BBCode URL Tag Cross-Site Scripting
- phpGraphy Cross-Site Scripting
- phpLDAPadmin Include File
- phpWebNotes Arbitrary Code Execution
- **PostNuke Multiple Cross-Site Scripting & SQL Injection (Updated)**
- **Beehive Forum SQL Injection or Cross Site Scripting (Updated)**
- QNX RTOS Information Disclosure
- ScriptsCenter AutoLinks Pro Include File Remote Arbitrary Code Execution
- WebCalendar 'Send_Reminders.PHP' Remote Code Execution
- YaPiG Cross-Site Scripting
- Cosmoshop SQL Injection & Information Disclosure

Wireless
Recent Exploit Scripts/Techniques
Trends
Viruses/Trojans

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
BFCommand & Control Software BFCommand & Control Server Manager 1.22_A & prior BFCommand & Control Vietman Server Manager 2.00_A & prior, 2.14_B	Multiple vulnerabilities have been reported in BFCommand & Control Server Manager and BFCommand & Control Vietman Server Manager that could let remote malicious users cause a Denial of Service or obtain elevated privileges. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	BFCommand & Control Server Managers Multiple Vulnerabilities	Medium	Secunia, Advisory: SA16629, August 30, 2005
Home FTP Server Home FTP Server r1.0.7 b45	A Directory Traversal vulnerability has been reported in Home FTP Server that could let remote malicious users access arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required.	Home FTP Server Arbitrary File Access CAN-2005-2726	Medium	Secunia, Advisory: SA16556, August 25, 2005

Leapware LeapFTP 2.7.0 to 2.7.5	A buffer overflow vulnerability has been reported in LeapFTP that could let local malicious users execute arbitrary code. Upgrade to version 2.7.6: http://www.leapware.com/ download.html There is no exploit code required; however, a Proof of Concept exploit script has been published.	LeapFTP Arbitrary Code Execution	High	Security Tracker, Alert ID: 1014785, August 24, 2005
Mercora IMRadio 1.0_pre7, 1.0_pre6-r4, 1.0pre6-3.3.5-20050130	A vulnerability has been reported in IMRadio that could let local malicious users disclose password information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	IMRadio Password Disclosure	Medium	Security Tracker, Alert ID: 1014780, August 24, 2005
Microsoft Internet Explorer 5.5, 6	A vulnerability has been reported in Internet Explorer ('msdds.dll' COM Object) that could let remote malicious users execute arbitrary code. Vendor workarounds available: http://www.microsoft.com/ technet/security/ advisory/906267.mspx **Advisory update to specify additional versions of 'msdds.dll' and to include additional mitigating factors.** An exploit script has been published.	Microsoft Internet Explorer Arbitrary Code Execution CAN-2005-2127	High	Microsoft Security Advisory 906267, August 18, 2005 US-CERT VU#740372 **Microsoft Security Advisory 906267, August 25, 2005**
Symantec Symantec AntiVirus Corporate Edition 9.0, 9.0.1, 9.0.2 Symantec Client Security 2.0.1, 2.0.2	A vulnerability has been reported in Symantec AntiVirus Corporate Edition and Symantec Client Security (help function) that could let local malicious users obtain elevated privileges. Vendor fix available: http://securityresponse.symantec.com /avcenter/security/Content /2005.08.24.html There is no exploit code required.	Symantec AntiVirus Corporate Edition and Client Security Privilege Elevation CAN-2005-2017	Medium	Symantec Security Response, ID: SYM05-012, August 24, 2005
TechWhale Solutions BlueWhaleCRM 1.0, 1.0.2	A vulnerability has been reported in BlueWhaleCRM that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required.	BlueWhaleCRM SQL Injection	Medium	Security Focus, ID: 14697, August 30, 2005
ZipTorrent ZipTorrent 1.3.7.3	A vulnerability has been reported in ZipTorrent that could let local malicious users disclose password information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	ZipTorrent Password Disclosure	Medium	Secunia, Advisory: SA16542, August 24, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Alexis Sukrieh Backup Manager 0.5.6, 0.5.7	A vulnerability has been reported because archives are created with insecure permissions, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://www.sukria.net/packages/ backup-manager/sources/ backup-manager-0 .5.8.tar.gz **Debian:** **http://security.debian.org/** **pool/updates/main/** **b/backup-manager/** There is no exploit code required.	Alexis Sukrieh Backup Manager Information Disclosure CAN-2005-1958	Medium	Security Tracker Alert, 1014124, June 7, 2005 **Debian Security Advisory, DSA 787-1, August 26, 2005**
Astaro Security Astaro Security Linux 6.0 01	A vulnerability has been reported due to a weakness that may allow remote malicious user to connect to arbitrary ports which could lead to access control bypass.	Astaro Security Linux HTTP CONNECT	Medium	Security Focus Bugtraq ID: 14665, August 25, 2005

	This issue was reportedly fixed by the vendor in Astaro Security Linux 6.002 There is no exploit code required; however, a Proof of Concept exploit has been published.	Unauthorized Access CAN-2005-2729		
BlueZ BlueZ 2.18 & prior	A vulnerability has been reported due to insufficient sanitization of input passed as a remote device name, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.bluez.org/redirect.php?url=http%3A%2F%2Fbluez.sf.net%2Fdown load%2Fbluez-libs-2.19.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200508-09.xml Debian: http://security.debian.org/pool/updates/contrib/b/bluez-utils/ **Mandriva:** **http://www.mandriva.com/security/advisories** There is no exploit code required.	BlueZ Arbitrary Command Execution CAN-2005-2547	High	Security Focus 14572, August 16, 2005 Gentoo Linux Security Advisory, GLSA 200508-09, August 17, 2005 Debian Security Advisory, DSA 782-1, August 23, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:150, August 25, 2005**
bzip2 bzip2 1.0.2	A remote Denial of Service vulnerability has been reported when processing malformed archives. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/b/bzip2/ Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SUSE: ftp://ftp.SUSE.com/pub/SUSE OpenPKG: http://www.openpkg.org/security/OpenPKG-SA-2005.008-openpkg.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-474.html FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:14/bzip2.patch Conectiva: ftp://atualizacoes.conectiva. com.br/ Debian: http://security.debian.org/pool/updates/main/b/bzip2/ SGI: http://www.sgi.com/support/security/ **IPCop:** **http://sourceforge.net/project/showfiles.php?group_id=40604&package_id = 35093&release_id=351848** Currently we are not aware of any exploits for this vulnerability.	bzip2 Remote Denial of Service CAN-2005-1260	Low	Ubuntu Security Notice, USN-127-1, May 17, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:091, May 19, 2005 Turbolinux Security Advisory, TLSA-2005-60, June 1, 2005 SUSE Security Summary Report, SUSE-SR:2005:015, June 7, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.008, June 10, 2005 RedHat Security Advisory, RHSA-2005:474-15, June 16, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:14, June 29, 2005 Conectiva Linux Announce-ment, CLSA-2005:972, July 6, 2005 Debian Security Advisory, DSA 741-1, July 7, 2005 SGI Security Advisory, 20050605-01-U, July 12, 2005 **Security Focus, Bugtraq ID: 13657, August 26, 2005**

Double Precision Incorporated Courier Mail Server 0.50	A remote Denial of Service vulnerability has been reported in the 'spf.c' source file when processing Sender Policy Framework (SPF) data. Upgrade available at: http://prdownloads. sourceforge.net/ courier/courier-0.50.1.tar.bz2?down load **Debian:** **http://security.debian.org/** **pool/updates/main/** **c/courier/** **Ubuntu:** **http://security.ubuntu.com/** **ubuntu/pool/main/c/courier/** Currently we are not aware of any exploits for this vulnerability.	Courier Mail Server Remote Denial of Service CAN-2005-2151	Low	Secunia Advisory: SA15901, July 4, 2005 **Debian Security Advisory, DSA 784-1, August 25, 2005** **Ubuntu Security Notice, USN-174-1, August 26, 2005**
Elm Development Group ELM 2.5.5-2.5.7	A buffer overflow vulnerability has been reported due to insufficient parsing of SMTP 'Expires' header lines, which could let a remote malicious user execute arbitrary code. Update to Elm 2.5 PL8 available at: ftp://ftp.virginia.edu /pub/elm/ **RedHat:** **http://rhn.redhat.com/** **errata/RHSA** **-2005-755.html** **A Proof of Concept exploit script has been published.**	Elm 'Expires' Header Remote Buffer Overflow CAN-2005-2665	High	Security Tracker Alert ID: 1014745, August 20, 2005 **RedHat Security Advisory, RHSA-2005:755-07, August 23, 2005**
FreeRADIUS Server Project FreeRADIUS 1.0.2	Two vulnerabilities have been reported: a vulnerability was reported in the 'radius_xlat()' function call due to insufficient validation, which could let a remote malicious user execute arbitrary SQL code; and a buffer overflow vulnerability was reported in the 'sql_escape_func()' function, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/ glsa/glsa-200505-13.xml SuSE: ftp://ftp.suse.com/pub/suse/ FreeRadius: ftp://ftp.freeradius.org/pub/ radius/freeradius-1.0.3.tar.gz RedHat: http://rhn.redhat.com/ errata/RHSA-2005-524.html SGI: http://www.sgi.com/ support/security/ **Fedora:** **http://download.fedora.** **redhat.com/pub/fedora/** **linux/core/updates/3** There is no exploit code required.	FreeRadius 'rlm_sql.c' SQL Injection & Buffer Overflow CAN-2005-1454 CAN-2005-1455	High	Security Tracker Alert ID: 1013909, May 6, 2005 Gentoo Linux Security Advisory, GLSA 200505-13, May 17, 2005 SUSE Security Summary Report, SUSE-SR:2005:014, June 7, 2005 Security Focus, 13541, June 10, 2005 RedHat Security Advisory, RHSA-2005: 524-05, June 23, 2005 SGI Security Advisory, 20050606- 01-U, July 12, 2005 **Fedora Update Notification,** **FEDORA-2005-807 August 25, 2005**
GNU shtool 2.0.1 & prior	A vulnerability has been reported that could let a local malicious user gain escalated privileges. The vulnerability is caused due to temporary files being created insecurely. Gentoo: http://security.gentoo.org/ glsa/glsa-200506-08.xml OpenPKG: ftp://ftp.openpkg.org/ release/2.3 RedHat: http://rhn.redhat.com/errata/ RHSA-2005-564.html Trustix: http://http.trustix.org/ pub/trustix/updates/ SGI:	GNU shtool Insecure Temporary File Creation CAN-2005-1751	Medium	Secunia Advisory, SA15496, May 25, 2005 Gentoo Linux Security Advisory, GLSA 200506 -08, June 11, 200 OpenPKG Security Advisory, OpenPKG-SA-2005.011, June 23, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005- 0036, July 14, 2005 SGI Security Advisory, 20050703-01-U, July 15, 2005

	http://www.sgi.com/support/security/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ **Debian:** **http://security.debian.org/pool/updates/main/p/php4/** There is no exploit code required.			Ubuntu Security Notice, USN-171-1, August 20, 2005 **Debian Security Advisory, DSA 789-1, August 29, 2005**
Hewlett Packard Company HP-UX B.11.23, B.11.11, B.11.00	A vulnerability has been reported in systems running the Veritas File System (VxFS), which could let a malicious user obtain sensitive information. Patches information available at: www2.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01218 Currently we are not aware of any exploits for this vulnerability.	HP-UX Veritas File System Information Disclosure	Medium	HP Security Bulletin, HPSBUX01218, August 24, 2005
Inter7 SqWebMail 5.0.4, 5.0 .1, 5.0.0, 4.0.5 -4.0.7, 4.0.4.20040524, 3.6.1, 3.6 .0, 3.5.0-3.5.3 , 3.4.1	A vulnerability has been reported due to insufficient sanitization of HTML emails, which could let a remote malicious user execute arbitrary HTML and script code. Updates available at: http://www.courier-mta.org/?download.php There is no exploit code required; however, a Proof of Concept exploit has been published.	SqWebMail HTML Email Arbitrary Code Execution	Medium	Secunia Advisory: SA16600, August 29, 2005
lm_sensors lm_sensors 2.9.1	A vulnerability has been reported in the 'pwmconfig' script due to the insecure creation of temporary files, which could result in a loss of data or a Denial of Service. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lm-sensors/ **Mandriva:** **http://www.mandriva.com/security/advisories** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200508-19.xml** There is no exploit code required.	LM_sensors PWMConfig Insecure Temporary File Creation CAN-2005-2672	Low	Security Focus, Bugtraq ID: 14624, August 22, 2005 Ubuntu Security Notice, USN-172-1, August 23, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:149, August 25, 2005** **Gentoo Linux Security Advisory, GLSA 200508-19, August 30, 2005**
maildrop maildrop 1.5.3	A vulnerability has been reported in lockmail, which could let a malicious user obtain elevated privileges. Debian: http://security.debian.org/pool/updates/main/m/maildrop/ There is no exploit code required.	Maildrop Lockmail Privilege Elevation CAN-2005-2655	Medium	Debian Security Advisory, DSA 791-1, August 30, 2005
Mike Kershaw Kismet 2005-07-R1	Multiple vulnerabilities have been reported: an integer underflow vulnerability was reported when handling pcap files; a vulnerability was reported due to an unspecified error when handling non-printable characters in SSID; and a integer underflow vulnerability was reported in the data frame dissection, which could possibly lead to the execution of arbitrary code. Upgrade available at: http://www.kismetwireless.net/code/kismet-2005-08-R1.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200508-10.xml **Debian:** **http://security.debian.org/pool/updates/main/k/kismet/**	Kismet Multiple Remote Vulnerabilities CAN-2005-2626 CAN-2005-2627	High	Security Focus, Bugtraq ID 14430, August 16, 2005 Gentoo Linux Security Advisory, GLSA 200508-10, August 19, 200 **Debian Security Advisory, DSA 788-1, August 29, 2005**

	Currently we are not aware of any exploits for these vulnerabilities.			
MPlayer MPlayer 1.0 pre7, .0 pre6-r4, 1.0 pre6-3.3.5-20050130	A buffer overflow vulnerability has been reported due to insufficient validation of user-supplied strings, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	MPlayer Audio Header Buffer Overflow CAN-2005-2718	High	Security Tracker Alert ID: 1014779, August 24, 2005
Multiple Vendors OpenLDAP 2.1.25; Padl Software pam_ldap Builds 166, 85, 202, 199, 198, 194, 183-192, 181, 180, 173, 172, 122, 121, 113, 107, 105	A vulnerability has been reported in OpenLDAP, 'pam_ldap,' and 'nss_ldap' when a connection to a slave is established using TLS and the client is referred to a master, which could let a remote malicious user obtain sensitive information. Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200507-13.xml Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/libn/ **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** There is no exploit code required.	Multiple Vendors TLS Plaintext Password CAN-2005-2069	Medium	Trustix Secure Linux Advisory, TSLSA-2005-0031, July 1, 2005 Gentoo Linux Security Advisory, GLSA 200507-13, July 14, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:121, July 19, 2005 Ubuntu Security Notice, USN-152-1, July 21, 2005 **Turbolinux Security Advisory, TLSA-2005-86 & 87, August 29, 2006**
Multiple Vendors RedHat Fedora Core3; LBL tcpdump 3.9.1, 3.9, 3.8.1-3.8.3, 3.7-3.7.2, 3.6.3, 3.6.2, 3.5.2, 3.5, alpha, 3.4, 3.4 a6	A remote Denial of Service vulnerability has been reported in the 'bgp_update_print()' function in 'print-bgp.c' when a malicious user submits specially crafted BGP protocol data. Update available at: http://cvs.tcpdump.org/cgi-bin/cvsweb/tcpdump/print-bgp.c Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/t/tcpdump/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Slackware: ftp://ftp.slackware.com/pub/slackware **IPCop:** **http://sourceforge.net/project/showfiles.php?group_id=40604&package_id = 35093&release_id=351848** A Proof of Concept exploit script has been published.	TCPDump BGP Decoding Routines Denial of Service CAN-2005-1267	Low	Security Tracker Alert, 1014133, June 8, 2005 Fedora Update Notification, FEDORA-2005-406, June 9, 2005 Trustix Secure Linux Security Advisory, TLSA-2005-0028, June 13, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:101, June 15, 2005 Fedora Update Notification, FEDORA-2005-407, June 16, 2005 Ubuntu Security Notice, USN-141-1, June 21, 2005 Turbolinux Security Advisory, TLSA-2005-69, June 22, 2005 Slackware Security Advisory, SSA:2005-195-10, July 15, 2005 **Security Focus, Bugtraq ID: 13906, August 26, 200-5**

Multiple Vendors zlib 1.2.2, 1.2.1, 1.2 .0.7, 1.1-1.1.4, 1.0-1.0.9; Ubuntu Linux 5.0 4, powerpc, i386, amd64, 4.1 ppc, ia64, ia32; SuSE Open-Enterprise-Server 9.0, Novell Linux Desktop 9.0, Linux Professional 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Personal 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Enterprise Server 9; Gentoo Linux; FreeBSD 5.4, -RELENG, -RELEASE, -PRERELEASE, 5.3, -STABLE, -RELENG, -RELEASE; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; zsync 0.4, 0.3-0.3.3, 0.2-0.2.3 , 0.1-0.1.6 1, 0.0.1-0.0.6	A buffer overflow vulnerability has been reported due to insufficient validation of input data prior to utilizing it in a memory copy operation, which could let a remote malicious user execute arbitrary code. Debian: ftp://security.debian.org/pool/updates/main/z/zlib/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:16/zlib.patch Gentoo: http://security.gentoo.org/glsa/glsa-200507-05.xml SUSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zlib/ Mandriva: http://www.mandriva.com/security/advisories OpenBSD: http://www.openbsd.org/errata.html OpenPKG: ftp.openpkg.org RedHat: http://rhn.redhat.com/errata/RHSA-2005-569.html Trustix: http://http.trustix.org/pub/trustix/updates/ Slackware: ftp://ftp.slackware.com/pub/slackware/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ zsync: http://prdownloads.sourceforge.net/zsync/zsync-0.4.1.tar.gz?download Apple: http://docs.info.apple.com/article.html?artnum=302163 SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.33 **IPCop:** **http://sourceforge.net/project/showfiles.php?group_id=40604&package_id = 35093&release_id=351848** Currently we are not aware of any exploits for this vulnerability.	Zlib Compression Library Buffer Overflow CAN-2005-2096	High	Debian Security Advisory DSA 740-1, July 6, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:16, July 6, 2005 Gentoo Linux Security Advisory, GLSA 200507-05, July 6, 2005 SUSE Security Announcement, SUSE-SA:2005:039, July 6, 2005 Ubuntu Security Notice, USN-148-1, July 06, 2005 RedHat Security Advisory, RHSA-2005:569-03, July 6, 2005 Fedora Update Notifications, FEDORA-2005-523, 524, July 7, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:11, July 7, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.013, July 7, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0034, July 8, 2005 Slackware Security Advisory, SSA:2005-189-01, July 11, 2005 Turbolinux Security Advisory, TLSA-2005-77, July 11, 2005 Fedora Update Notification, FEDORA-2005-565, July 13, 2005 SUSE Security Summary Report, SUSE-SR:2005:017, July 13, 2005 Security Focus, 14162, July 21, 2005 USCERT Vulnerability Note VU#680620, July 22, 2005 Apple Security Update 2005-007, APPLE-SA-2005-08-15, August 15, 2005 SCO Security Advisory, SCOSA-2005.33, August 19, 2005 **Security Focus, Bugtraq ID: 14162, August 26, 2005**

Multiple Vendors dhcpcd 1.3.22	A vulnerability has been reported in dhcpcd that could let a remote user perform a Denial of Service. Debian: http://security.debian.org/ pool/updates/main/d/dhcpcd/ Mandriva: http://www.mandriva.com/ security/advisories Gentoo: http://security.gentoo.org/ glsa/glsa-200507-16.xml Conectiva: http://distro.conectiva.com.br/ atualizacoes/ index.php ?id=a& anuncio=000983 RedHat: http://rhn.redhat.com/ errata/RHSA-2005-603.html Debian: http://security.debian.org/ pool/updates/main/ **IPCop:** **http://sourceforge.net/project/** **showfiles.php?group_id=** **40604&package_id =** **35093&release_id=351848** Currently we are not aware of any exploits for this vulnerability.	dhcpcd Denial of Service CAN-2005-1848	Low	Secunia, Advisory: SA15982, July 11, 2005 Debian Security Advisory, DSA 750-1, July 11, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:117, July 13, 2005 Gentoo Linux Security Advisory, GLSA 200507-16, July 15, 2005 Conectiva, CLSA-2005:983, July 25, 2005 RedHat Security Advisory, RHSA-2005:603-07, July 27, 2005 Debian Security Advisor, DSA 773-1, August 11, 2005 **Security Focus, Bugtraq ID: 14206 , August 26, 2005**
Multiple Vendors Linux kernel 2.6 -2.6.13	A Denial of Service vulnerability has been reported when processing specially crafted ELF headers on 64 bit x86 platforms. Updates available at: http://kernel.org/pub/linux/ kernel/v2.6/testing/ ChangeLog-2.6.13-rc4 Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 64 Bit ELF Header Denial of Service CAN-2005-2617	Low	Security Focus, Bugtraq ID: 14661, August 25, 2005
Multiple Vendors Linux kernel 2.6-2.6.12 .1	A vulnerability has been reported due to insufficient authorization before accessing a privileged function, which could let a malicious user bypass IPSEC policies. Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/l/ **This issue has been addressed in Linux kernel 2.6.13-rc7.** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel IPSec Policies Authorization Bypass CAN-2005-2555	Medium	Ubuntu Security Notice, USN-169-1, August 19, 2005 Security Focus, Bugtraq ID 14609, August 19, 2005 **Security Focus, Bugtraq ID 14609, August 25, 2005**
Multiple Vendors Simpleproxy 3.0-3.2 , 2.2b; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	A format string vulnerability has been reported when handling HTTP proxy replies, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://prdownloads.sourceforge. net/simpleproxy/simpleproxy- 3.4.tar.gz? download Debian: http://security.debian.org/ pool/updates/main/s/ simpleproxy/ Currently we are not aware of any exploits for this vulnerability.	Simpleproxy HTTP Proxy Reply Format String CAN-2005-1857	High	Debian Security Advisory, DSA 786-1, August 26, 2005
Multiple Vendors Turbolinux Server 10.0, 8.0, Desktop 10.0, Turbolinux Home Appliance Server 1.0 Workgroup Edition, Hosting Edition; Trustix Secure Linux 3.0, 2.2, Secure Enterprise	Multiple vulnerabilities have been reported: a remote Denial of Service vulnerability was reported when a malicious user submits a specially crafted TCP connection that causes the Key Distribution Center (KDC) to attempt to free random memory; a buffer overflow vulnerability was reported in KDC due to a boundary error when a specially crafted TCP or UDP request is submitted, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported in 'krb/recvauth.c' which could let a remote malicious user execute arbitrary code.	Kerberos V5 Multiple Vulnerabilities CAN-2005-1174 CAN-2005-1175 CAN-2005-1689	High	MIT krb5 Security Advisory, 2005-002, July 12, 2005 RedHat Security Advisory, RHSA-2005:567-08, July 12, 2005 Sun(sm) Alert Notification, 101809, July 12, 2005

Linux 2.0; Sun Solaris 10.0 _x86, 10.0, 9.0 _x86 Update 2, 9.0 _x86, 9.0, Sun SEAM 1.0-1.0.2; SuSE Linux Professional 9.3 x86_64, 9.3, Linux Personal 9.3 x86_64, 9.3; RedHat Fedora Core3 & 4, Advanced Workstation for the Itanium Processor 2.1; MIT Kerberos 5 5.0 -1.4.1 & prior; Gentoo Linux	MIT: http://web.mit.edu/kerberos/advisories/2005-002-patch_1.4.1.txt.asc Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates RedHat: http://rhn.redhat.com/errata/RHSA-2005-567.html Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101809-1 SuSE: http://www.novell.com/linux/security/advisories.html Trustix: http://http.trustix.org/pub/trustix/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SGI: http://www.sgi.com/support/security/ Debian: http://www.debian.org/security/2005/dsa-757 Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000993 **Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101810-1** Currently we are not aware of any exploits for these vulnerabilities.		Fedora Update Notifications, FEDORA-2005-552 & 553, July 12, 2005 SUSE Security Summary Report, SUSE-SR:2005:017, July 13, 2005 Turbolinux Security Advisory TLSA-2005-78, July 13, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:119, July 14, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0036, July, 14, 2005 SGI Security Advisory, 20050703-01-U, July 15, 2005 Debian Security Advisory, DSA-757-1, July 17, 2005 US-CERT VU#885830 US-CERT VU#623332 US-CERT VU#259798 Conectiva Linux Advisory, CLSA-2005:993, August 8, 2005 **Sun(sm) Alert Notification Sun Alert ID: 101810, August 29, 2005**

Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; GNOME Evolution 2.3.1 -2.3.6 .1, 2,0-2.2 , 1.5	Multiple format string vulnerabilities have been reported: a vulnerability was reported when vCard information is attached to an email message, which could let a remote malicious user execute arbitrary code; a vulnerability was reported when specially crafted contact data that has been retrieved from an LDAP server is displayed, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported when specially crafted task list data that has been retrieved from remote servers and the data that has been saved under the 'Calendars' tab is displayed, which could let a remote malicious user execute arbitrary code. Updates available at: http://ftp.gnome.org/pub/gnome/sources/evolution/2.3/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/evolution/ Mandriva: http://www.mandriva.com/security/advisories SUSE: ftp://ftp.suse.com/pub/suse/ Gentoo: http://security.gentoo.org/glsa/glsa-200508-12.xml **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-267.html** Currently we are not aware of any exploits for these vulnerabilities.	GNOME Evolution Multiple Format String CAN-2005-2549 CAN-2005-2550	High	Secunia Advisory: SA16394, August 11, 2005 Ubuntu Security Notice, USN-166-1, August 11, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:141, August 18, 2005 SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005 Gentoo Linux Security Advisory, GLSA 200508-12, August 23, 200 **RedHat Security Advisory, RHSA-2005:267-10, August 29, 2005**

Multiple Vendors X.org X11R6 6.7.0, 6.8, 6.8.1; XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0, 4.0.1, 4.0.2 -11, 4.0.3, 4.1.0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1, 4.3.0.2, 4.3.0.1, 4.3.0	An integer overflow vulnerability exists in 'scan.c' due to insufficient sanity checks on on the 'bitmap_unit' value, which could let a remote malicious user execute arbitrary code. Patch available at: https://bugs.freedesktop.org/attachment.cgi?id=1909 Gentoo: http://security.gentoo.org/glsa/glsa-200503-08.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lesstif1-1/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-15.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/x/xfree86/ ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-331.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-044.html Mandrake: http://www.mandrakesecure.net/en/ftp.php Mandriva: http://www.mandriva.com/security/advisories Debian: http://security.debian.org/pool/updates/main/x/xfree86/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-412.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-473.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-198.html Apple: http://docs.info.apple.com/article.html?artnum=302163 **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Currently we are not aware of any exploits for this vulnerability.	LibXPM Bitmap_unit Integer Overflow CAN-2005-0605	High	Security Focus, 12714, March 2, 2005 Gentoo Linux Security Advisory, GLSA 200503-08, March 4, 2005 Ubuntu Security Notice, USN-92-1 March 07, 2005 Gentoo Linux Security Advisory, GLSA 200503-15, March 12, 2005 Ubuntu Security Notice, USN-97-1 March 16, 2005 ALTLinux Security Advisory, March 29, 2005 Fedora Update Notifications, FEDORA-2005 -272 & 273, March 29, 2005 RedHat Security Advisory, RHSA-2005: 331-06, March 30, 2005 SGI Security Advisory, 20050401-01-U, April 6, 2005 RedHat Security Advisory, RHSA-2005:044-15, April 6, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:080, April 29, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:081, May 6, 2005 Debian Security Advisory, DSA 723-1, May 9, 2005 RedHat Security Advisory, RHSA-2005:412-05, May 11, 2005 RedHat Security Advisory, RHSA-2005:473-03, May 24, 2005 RedHat Security Advisory, RHSA-2005:198-35, June 8, 2005 **Fedora Update Notifications, FEDORA-2005-808 & 815, August 25 & 26, 2005**

Nokia Affix 3.0-3.2, 2.1-2.1.2, 2.0 -2.0.2	A vulnerability has been reported in the 'event_pin_code_request()' function due to an input validation error, which could let a remote malicious user inject arbitrary shell commands via a specially crafted Bluetooth device name. Patches available at: http://affix.sourceforge.net/patch_btsrv_affix_2_1_2 http://affix.sourceforge.net/patch_btsrv_affix_3_2_0 There is no exploit code required.	Nokia Affix BTSRV Device Name Remote Command Execution CAN-2005-2716	High	DMA 2005-0826a Advisory, August 26, 2005
Padl Software pam_ldap Build 179, Build 169	A vulnerability has been reported when handling a new password policy control, which could let a remote malicious user bypass authentication policies. Upgrades available at: ftp://ftp.padl.com/pub/pam_ldap.tgz There is no exploit code required.	PADL Software PAM_LDAP Authentication Bypass CAN-2005-2641	Medium	Bugtraq ID: 14649, August 24, 2005 US-CERT VU#778916
PCRE PCRE 6.1, 6.0, 5.0	A vulnerability has been reported in 'pcre_compile.c' due to an integer overflow, which could let a remote/local malicious user potentially execute arbitrary code. Updates available at: http://www.pcre.org/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/pcre3/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200508-17.xml** **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	PCRE Regular Expression Heap Overflow CAN-2005-2491	High	Secunia Advisory: SA16502, August 22, 2005 Ubuntu Security Notice, USN-173-1, August 23, 2005 **Ubuntu Security Notices, USN-173-1 & 173-2, August 24, 2005** **Fedora Update Notifications, FEDORA-2005-802 & 803, August 24, 2005** **Gentoo Linux Security Advisory, GLSA 200508-17, August 25, 2005** **Mandriva Linux Security Update Advisories, MDKSA-2005:151-155, August 25, 26, & 29, 2005**
PHP Arena paFileDB 3.1	An SQL injection vulnerability has been reported in 'auth.php' due to insufficient sanitization of the 'user' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PAFileDB 'Auth.PHP' SQL Injection CAN-2005-2723	Medium	SePro Advisory #5, August 24, 2005
phpMyAdmin phpMyAdmin 2.6 .0-2.6.3, 2.5 .0-2.5.7, 2.4 .0, 2.3.2, 2.3.1, 2.2 -2.2.6, 2.1-2.1 .2, 2.0-2.0.5	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability has been reported in 'libraries/auth/cookie.auth.lib.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability has been reported in 'error.php' due to insufficient sanitization of the 'error' parameter, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=23067 There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPMyAdmin Cross-Site Scripting	Medium	Secunia Advisory: SA16605, August 29, 2005

RedHat Fedora Core3	A vulnerability has been reported in xntpd when started using the '-u' option and the group is specified by a string, which could let a malicious user obtain elevated privileges. Upgrade available at: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/i386 /ntp-4.2.0.a.20040617-5.FC3.i386.rpm There is no exploit code required.	XNTPD Insecure Privileges CAN-2005-2496	Medium	Fedora Update Notification, FEDORA-2005-812, August 26, 2005
slocate slocate 2.7	A Denial of Service vulnerability has been reported when a specially crafted directory structure that contains long paths is submitted. Mandriva: http://www.mandriva.com/security/advisories There is no exploit code required.	slocate Long Path Denial of Service CAN-2005-2499	Low	Mandriva Linux Security Update Advisory, MDKSA-2005:147, August 22, 2005
Sun Microsystems, Inc. Messaging Server 6.2, iPlanet Messaging Server 5.2	A vulnerability has bee reported in in Sun ONE Messaging Server (iPlanet Messaging Server), which could let a remote malicious user execute arbitrary code. *Note: Only target users running Internet Explorer are affected.* **Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101770-1** There is no exploit code required.	Sun ONE/iPlanet Messaging Server Arbitrary Code Execution CAN-2005-2022	High	Sun(sm) Alert Notification, 101770, June 17, 2005 **Sun(sm) Alert Notification, 101770, August 25, 2005**
Sun Microsystems, Inc. Solaris 10.0 _x86, 10.0	A vulnerability has been reported in the '/lib/svc/method/net-svc' script, which could let a remote malicious user execute arbitrary code on the DHCP client system with ROOT privileges. Patches available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101897-1 Currently we are not aware of any exploits for this vulnerability.	Sun Solaris DHCP Client Remote Code Execution	High	Sun(sm) Alert Notification Sun Alert ID: 101897, August 23, 2005
Tor Tor 0.1.0.13 & prior	A vulnerability has been reported when performing a Diffie-Hellman handshake due to a failure to reject certain weak keys, which could let a remote malicious user obtain sensitive information. Update available at: http://tor.eff.org/download.html **Gentoo: http://security.gentoo.org/glsa/glsa-200508-16.xml** Currently we are not aware of any exploits for this vulnerability.	Tor Weak Diffie-Hellman Handshake CAN-2005-2643	Medium	Secunia Advisory: SA16424, August 19, 2005 **Gentoo Linux Security Advisory, GLSA 200508-16, August 25, 2005**
University of Minnesota gopherd 3.0.9	A buffer overflow vulnerability has been reported in the 'VlfromLine()' function when copying an input line, which could let a remote malicious user obtain unauthorized access. No workaround or patch available at time of publishing. An exploit script has been published.	UMN Gopher Client Remote Buffer Overflow	Medium	Secunia Advisory: SA16614, August 30, 2005

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Alexander Palmo Simple PHP Blog 0.4	A Directory Traversal vulnerability has been reported in 'Comment_Delete_cgi.php' due to insufficient sanitization which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, an exploit script has been published.	Simple PHP Blog Directory Traversal	Medium	Bugtraq ID: 14681, August 29, 2005

Alexander Palmo Simple PHP Blog 0.4	A vulnerability has been reported in 'upload_img_cgi.php' due to a failure to validate the extension of an uploaded image file, which could let a remote malicious user upload arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required.	Simple PHP Blog Remote Arbitrary File Upload CAN-2005-2733	Medium	Secunia Advisory: SA16598, August 26, 2005
All Enthusiast, Inc. PhotoPost Pro, 5.1	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of EXIF data stored in certain image files, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PhotoPost Cross-Site Scripting CAN-2005-2737	Medium	Security Tracker Alert ID: 1014803, August 26, 2005
CVS CVS 1.12.7-1.12.12, 1.12.5, 1.12.2 , 1.12.1, 1.11.19, 1.11.17	A vulnerability has been reported in the 'cvsbug.in' script due to the insecure creation of temporary files, which could let a malicious user cause data loss or a Denial of Service. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ There is no exploit code required.	CVS 'Cvsbug.In' Script Insecure Temporary File Creation CAN-2005-2693	Low	Fedora Update Notifications FEDORA-2005-790 & 791, August 23, 2005
De-Neef.net Looking Glass	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'footer.php' and 'header.php' due to insufficient sanitization of the 'version' array, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in 'lg.php' due to insufficient sanitization of the 'target' parameter before using in a 'system()' call, which could let a remote malicious user inject arbitrary shell commands. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Looking Glass Input Validation	High	Secunia Advisory: SA16607, August 29, 2005
e107.org e107 website system 0.617, 0.616, 0.603	A vulnerability has been reported in the 'forum_post.php' script due to insufficient verification if a forum exists when posting a message, which could let a remote malicious user create arbitrary forum message posts. No workaround or patch available at time of publishing. There is no exploit code required.	e107 Forum_post.PHP Non-existing Forums	Medium	Security Tracker Alert ID: 1014819, August 30, 2005
Flagship Industries Ventrilo 2.3, 2.2, 2.1.2-2.1.4	A remote Denial of Service vulnerability has been reported when handling certain malformed status query packets. No workaround or patch available at time of publishing. An exploit script has been published.	Ventrilo Status Requests Remote Denial of Service CAN-2005-2719	Low	Security Tracker Alert ID: 1014784 , August 24, 2005
Foojan PHP Weblog	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to the 'Referer' HTTP header before stored in the 'visits' table, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Foojan PHPWeblog Cross-Site Scripting CAN-2005-2721	Medium	Secunia Advisory: SA16565, August 25, 2005
FreeStyle Wiki Wiki 3.5.8	A vulnerability has been reported when validating certain input in the management page, which could let a remote malicious user execute arbitrary Perl commands. Upgrade available at: http://prdownloads.sourceforge.jp/fswiki/16170/wiki3_5_9.zip There is no exploit code required.	FreeStyle Wiki Arbitrary Perl Command Execution	Medium	Secunia Advisory: SA16612, August 30, 2005
Gallery Project Gallery 1.5.1 -RC2 & prior	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of EXIF data stored in certain image files, which could let a remote malicious user execute arbitrary HTML and script code. Updates available at: http://gallery.menalto.com/modules.php?op=modload&name=phpWiki&file=index&pagename=Download There is no exploit code required; however, a Proof of Concept exploit has been published.	Gallery Cross-Site Scripting CAN-2005-2734	Medium	Security Tracker Alert ID: 1014800, August 26, 2005

Helpdesk Software Hesk 0.92	A vulnerability has been reported due to insufficient validation of username and password pairs, which could let a remote malicious user bypass authentication and obtain administrative access. Update available at: http://www.phpjunkyard.com/download.php?script=hesk There is no exploit code required; however, a Proof of Concept exploit has been published.	Helpdesk Software Hesk Authentication Bypass	High	Security Focus, Bugtraq ID: 14692, August 29, 2005
Hewlett Packard Company OpenView Network Node Manager 7.50 Solaris, 7.50, 6.41 Solaris, 6.41	A vulnerability has been reported in the 'node' URI parameter of the 'OvCgi/connectedNodes.ovpl' script, which could let a remote malicious user execute arbitrary code. Workaround available at: http://support.openview.hp.com/news_archives.jsp There is no exploit code required; however, a Proof of Concept exploit script has been published.	HP OpenView Network Node Manager Remote Arbitrary Code Execution	High	Portcullis Security Advisory, 05-014, August 25, 2005 HP Security Advisory, HPSBMA01224, August 26, 2005
Ilia Alshanetsky FUDForum 2.6.15	A vulnerability has been reported in the 'mid' parameter due to insufficient validation before retrieving a forum post, which could let a remote malicious user bypass certain security restrictions and obtain sensitive information. **PHPGroupWare:** **http://prdownloads.sourceforge.net/phpgroupware/phpgroupware-0.9.16.00 7.tar.gz** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200508-20.xml** There is no exploit code required.	FUDForum Security Restriction Bypass CAN-2005-2600	Medium	Secunia Advisory: SA16414, August 12, 2005 **Security Focus, Bugtraq ID: 14556, August 25, 2005** **Gentoo Linux Security Advisory, GLSA 200508-20, August 30, 2005**
Ilia Alshanetsky FUDForum 2.7, 2.6.12 -2.6.15, 2.6.7 -2.6.10, 2.6-2.6.5	A vulnerability has been reported when an image file is merged with a script file and uploaded, which could let a remote malicious user obtain unauthorized access. No workaround or patch available at time of publishing. There is no exploit code required.	FUDforum Avatar Upload Arbitrary Script Upload	Medium	Security Focus, Bugtraq ID: 14678, August 29, 2005
Interspire ArticleLive 2005	A Cross-Site Scripting vulnerability has been reported in 'articles.newcomment' due to insufficient sanitization of the 'ArticleId' parameter, which could let a remote malicious user execute arbitrary HTML and script code. **Upgrade available at:** **http://www.interspire.com/articlelive/** There is no exploit code required; however, a Proof of Concept exploit has been published.	InterSpire ArticleLive NewComment Cross-Site Scripting CAN-2005-0881	High	Secunia Advisory, SA14708, March 23, 2005 **Security Focus, Bugtraq ID: 12879, August 23, 2005**
Jelsoft Enterprises vBulletin 3.0	A vulnerability has been reported in the 'backup.php' script due to insufficient password protection and encryption, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	vBulletin 'backup.php' Information Disclosure	Medium	Security Tracker Alert ID: 1014805, August 29, 2005
Lithium Software Lithium II Mod 1.24	A format string vulnerability has been reported when displaying the score at the end of the game, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Lithium Software Quake 2 Lithium II Mod Format String	High	Security Focus, Bugtraq ID: 14664, August 25, 2005
Mozilla.org Firefox 0.x, 1.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to an error because untrusted events generated by web content are delivered to the browser user interface; a vulnerability was reported because scripts in XBL controls can be executed even when JavaScript has been disabled; a vulnerability was reported because remote malicious users can execute arbitrary code by tricking the user into using the 'Set As Wallpaper' context menu on an image URL that is really a javascript; a vulnerability was reported in the 'InstallTrigger.install()' function due to an error in the callback function, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to an error when handling 'data:' URL that originates from the sidebar, which could let a remote malicious user execute arbitrary code; an input validation vulnerability was reported in the 'InstallVersion.compareTo()' function when handling unexpected JavaScript objects, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because it is possible for remote malicious user to steal information and possibly execute arbitrary code by using standalone applications such as Flash and QuickTime to open a javascript: URL; a vulnerability was reported due to an error when handling DOM node names with different namespaces, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported due to insecure cloning of base objects, which could let a remote malicious user execute	Firefox Multiple Vulnerabilities CAN-2005-2260 CAN-2005-2261 CAN-2005-2262 CAN-2005-2263 CAN-2005-2264 CAN-2005-2265 CAN-2005-2267 CAN-2005-2269 CAN-2005-2270	High	Secunia Advisory: SA16043, July 13, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:120, July 13, 2005 Gentoo Linux Security Advisory, GLSA 200507-14, July 15, 2005 Gentoo Linux Security Advisory, GLSA 200507-17, July 18,

	arbitrary code. Updates available at: http://www.mozilla.org/products/firefox/ Gentoo: ftp://security.gentoo.org/glsa/ **Mandriva:** **http://www.mandriva.com/security/advisories** Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates RedHat: http://rhn.redhat.com/errata/RHSA-2005-586.html Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005& m=slackware-security.418880 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/epiphany-browser/ http://security.ubuntu.com/ubuntu/pool/main/e/enigmail/ http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-thunderbird/ SUSE: ftp://ftp.suse.com/pub/suse/ Debian: http://security.debian.org/pool/updates/main/m/mozilla-firefox/ http://security.debian.org/pool/updates/main/m/mozilla/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200507-24.xml** **Slackware:** **ftp://ftp.slackware.com/pub/slackware/** Exploits have been published.			2005 Fedora Update Notifications, FEDORA-2005-603 & 605, July 20, 2005 RedHat Security Advisory, RHSA-2005:586-11, July 21, 2005 Slackware Security Advisory, SSA:2005-203-01, July 22, 2005 US-CERT VU#652366 US-CERT VU#996798 Ubuntu Security Notices, USN-155-1 & 155-2 July 26 & 28, 2005 Ubuntu Security Notices, USN-157-1 & 157-2 August 1& 2, 2005 SUSE Security Announcement, SUSE-SA:2005:045, August 11, 2005 Debian Security Advisory, DSA 775-1, August 15, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 Debian Security Advisory, DSA 777-1, August 17, 2005 Debian Security Advisory, DSA 779-1, August 20, 2005 Debian Security Advisory, DSA 781-1, August 23, 2005 **Gentoo Linux Security Advisory, GLSA 200507-24, August 26, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:127-1, August 26, 2005** **Slackware Security Advisory, SSA:2005-085-01, August 28, 2005**
Multiple Vendors Gentoo Linux; Apache Software Foundation Apache 2.1-2.1.5, 2.0.35-2.0.54, 2.0.32, 2.0.28, Beta, 2.0 a9, 2.0	A remote Denial of Service vulnerability has been reported in the HTTP 'Range' header due to an error in the byte-range filter. Patches available at: http://issues.apache.org/bugzilla/attachment.cgi?id=16102 Gentoo: http://security.gentoo.org/glsa/glsa-200508-15.xml There is no exploit code required.	Apache Remote Denial of Service CAN-2005-2728	Low	Secunia Advisory: SA16559, August 25, 2005 Security Advisory, GLSA 200508-15, August 25, 2005

Multiple Vendors PHPXMLRPC 1.1.1; PEAR XML_RPC 1.3.3; Drupal 4.6-4.6.2, 4.5- 4.5.4; Nucleus CMS Nucleus CMS 3.21, 3.2, 3.1, 3.0, RC, 3.0.; MailWatch for MailScanner 1.0.1; eGroupWare 1.0.6, 1.0.3, 1.0.1, 1.0.0.007, 1.0	A vulnerability has been reported in XML-RPC due to insufficient sanitization of certain XML tags that are nested in parsed documents being used in an 'eval()' call, which could let a remote malicious user execute arbitrary PHP code. PHPXMLRPC : http://prdownloads.sourceforge.net/phpxmlrpc/xmlrpc.1.2.tgz?download Pear: http://pear.php.net/get/XML_RPC-1.4.0.tgz Drupal: http://drupal.org/files/projects/drupal-4.5.5.tar.gz eGroupWare: http://prdownloads.sourceforge.net/egroupware/eGroupWare-1.0.0.009.tar .gz?download MailWatch: http://prdownloads.sourceforge.net/mailwatch/mailwatch-1.0.2.tar.gz Nucleus: http://prdownloads.sourceforge.net/nucleuscms/nucleus-xmlrpc-patch.zip ?download RedHat: http://rhn.redhat.com/errata/RHSA-2005-748.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Mandriva: http://www.mandriva.com/security/advisories **Gentoo:** **http://security.gentoo.org/glsa/glsa-200508-13.xml** **http://security.gentoo.org/glsa/glsa-200508-14.xml** **http://security.gentoo.org/glsa/glsa-200508-18.xml** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **Debian:** **http://security.debian.org/pool/updates/main/p/php4/** **SUSE:** **ftp://ftp.suse.com/pub/suse/** There is no exploit code required.	PHPXMLRPC and PEAR XML_RPC Remote Arbitrary Code Execution CAN-2005-2498	High	Security Focus, Bugtraq ID 14560, August 15, 2995 Security Focus, Bugtraq ID 14560, August 18, 2995 RedHat Security Advisory, RHSA-2005:748-05, August 19, 2005 Ubuntu Security Notice, USN-171-1, August 20, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:146, August 22, 2005 **Gentoo Linux Security Advisory, GLSA 200508-13 & 14, & 200508-18, August 24 & 26, 2005** **Fedora Update Notifications, FEDORA-2005-809 & 810, August 25, 2005** **Debian Security Advisory, DSA 789-1, August 29, 2005** **SUSE Security Announcement, SUSE-SA:2005:049, August 30, 2005**
Multiple Vendors Xoops 2.0.10-2.0.12, 2.0.9 .3, 2.0.9.2, 2.0.5-2.0.5.2, 2.0-2.0.3; XML-RPC for PHP XML-RPC for PHP 1.1, 1.0.99 .2, 1.0.99, 1.0-1.02; WordPress	A vulnerability was reported due to insufficient sanitization of the 'eval()' call, which could let a remote malicious user execute arbitrary PHP code. Drupal: http://drupal.org/files/projects/drupal-4.5.4.tar.gz Mandriva: http://www.mandriva.com/	Multiple Vendors XML-RPC for PHP Remote Code Injection CAN-2005-1921	High	Security Focus, 14088, June 29, 2005 Gentoo Linux Security Advisory, GLSA 200507-01, July 3, 2005 Fedora Update Notifications,

1.5-1.5.1 .2, 1.2-1.2.2, 0.71,0.7; S9Y Serendipity 0.8.1, 0.8 -beta6 Snapshot, 0.8 -beta5 & beta6, 0.8; PostNuke Development Team PostNuke 0.76 RC4a&b, RC4, 0.75; phpMyFAQ 1.5 RC1-RC4, 1.5 beta1-beta3, 1.5 alpha1&2, 1.4-1.4.8, 1.4; PEAR XML_RPC 1.3 RC1-RC3, 1.3; MandrakeSoft Linux Mandrake 10.2 x86_64, 10.2, 10.1 x86_64, 10.1 , 10.0 amd64, 10.0, Corporate Server 3.0 x86_64, 3.0; Drupal 4.6.1, 4.6, 4.5- 4.5.3	security/advisories Pear: http://pear.php.net/get/XML_RPC-1.3.1.tgz PhpMyFaq: http://freshmeat.net/redir/phpmyfaq/38789/url_zip/download.php S9Y Serendipity: http://prdownloads.sourceforge.net/php-blog/serendipity-0.8.2.tar.gz?d ownload Trustix: http://http.trustix.org/pub/trustix/updates/ WordPress: http://wordpress.org/latest.zip XML-RPC: http://prdownloads.sourceforge.net/phpxmlrpc/xmlrpc-1.1.1.tgz?download Xoops: http://www.xoops.org/modules/core/visit.php?cid=3&lid=62 Gentoo: http://security.gentoo.org/glsa/glsa-200507-01.xml http://security.gentoo.org/glsa/glsa-200507-06.xml http://security.gentoo.org/glsa/glsa-200507-07.xml http://security.gentoo.org/glsa/glsa-200507-15.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Debian: http://security.debian.org/pool/updates/main/d/drupal/ http://security.debian.org/pool/updates/main/p/phpgroupware/ http://security.debian.org/pool/updates/main/e/egroupware/ SGI: http://www.sgi.com/support/security/ SuSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: http://http.trustix.org/pub/trustix/updates/ **Debian:** **http://security.debian.org/pool/updates/main/p/php4/**		FEDORA-2005-517 & 518, July 5, 2006 Ubuntu Security Notice, USN-147-1 & USN-147-2, July 05 & 06, 2005 US-CERT VU#442845 Gentoo Linux Security Advisory, GLSA 200507-06, July 6, 2005 Gentoo Linux Security Advisory, GLSA 200507-07, July 10, 2005 SuSE Security Announcement, SUSE-SA:2005:041, July 8, 2005 Debian Security Advisories, DSA 745-1, 747-1, & DSA 746-1, July 10 & 13, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0036, July 14, 2005 SGI Security Advisory, 20050703-01-U, July 15, 2005 Gentoo Linux Security Advisory, GLSA 200507-15, July 15, 2005 **Debian Security Advisory, DSA 789-1, August 29, 2005** **SUSE Security Announcement, SUSE-SA:2005:049, August 30, 2005**

	SUSE: **ftp://ftp.suse.com** **/pub/suse/** Exploit scripts have been published.			
MyBB Group MyBulletinBoard RC1-RC4	An SQL injection vulnerability has been reported in the 'member.php' script due to insufficient validation of the 'fid' parameter, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	MyBB SQL Injection CAN-2005-2697	Medium	Security Tracker Alert ID: 1014806, August 29, 2005
MySQL AB MySQL 4.0 .0-4.0.11, 5.0 .0- 5.0.4	A vulnerability has been reported in the 'mysql_install_db' script due to the insecure creation of temporary files, which could let a malicious user obtain unauthorized access. Fedora: http://download.fedora. redhat.com/pub/fedora/ linux/core/updates/4/ **Debian:** **http://security.debian.** **org/pool/updates/** **main/m/mysql-** **dfsg-4.1/** There is no exploit code required.	MySQL 'mysql_install_db' Insecure Temporary File Creation CAN-2005-1636	Medium	Security Focus, 13660, May 17, 2005 Fedora Update Notification, FEDORA-2005-557, July 20, 2005 **Debian Security Advisory, DSA 783-1, August 24, 2005**
PHP-Fusion PHP-Fusion 6.0.107, 6.0.105, 6.0 106, 5.0 1 Service Pack, 5.0 , 4.0 1, 4.00	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of nested 'URL' bbcode tags before used in a post, which could let a remote malicious user execute arbitrary script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHP-Fusion BBCode URL Tag Cross-Site Scripting	Medium	Security Focus Bugtraq ID: 14688, August 29, 2005
phpGraphy phpGraphy 0.9.9 a	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of EXIF data stored in certain image files, which could let a remote malicious user execute arbitrary HTML and script code. Upgrade available at: http://prdownloads. sourceforge.net/ phpgraphy/phpgraphy- 0.9.10.tar.gz There is no exploit code required; however, a Proof of Concept exploit has been published.	phpGraphy Cross-Site Scripting CAN-2005-2735	Medium	Security Tracker Alert ID: 1014801, August 26, 2005
phpldapadmin phpldapadmin 0.9.6 - 0.9.7/alpha5	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported due to insufficient user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; a Directory Traversal vulnerability was reported which could let a remote malicious user obtain sensitive information; and a file include vulnerability was reported, which could let a remote malicious user execute arbitrary PHP script code. No workaround or patch available at time of publishing. There is no exploit code required; however; a Proof of Concept exploit has been published.	phpLDAPadmin Multiple Vulnerabilities	Medium	Security Focus, Bugtraq ID: 14695, August 30, 2005
phpWebNotes phpWebNotes 2.0	A vulnerability has been reported in the 'php_api.php' script due to insufficient validation of the 't_path_core' parameter, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	phpWebNotes Arbitrary Code Execution	High	Security Tracker Alert ID: 1014807, August 29, 2005
PostNuke Development Team PostNuke 0.76 RC4b	Multiple vulnerabilities have been reported: Cross-Site Scripting vulnerabilities were reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported in 'DL-viewdownload.PHP' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code. **Upgrades available at:** **http://news.postnuke.com/** **Downloads-req-** **getit-lid-480.html** There is no exploit code required; however, a Proof of Concept exploit has been published.	PostNuke Multiple Cross-Site Scripting & SQL Injection CAN-2005-2689 CAN-2005-2690	Medium	Security Focus Bugtraq ID: 14635 & 14636, August 22, 2005 **Security Focus Bugtraq ID: 14635 & 14636, August 25, 2005**
Project: Beehive Forum Beehive Forum	Multiple vulnerabilities have been reported in Beehive Forum that could allow remote malicious users to perform SQL injection or Cross-Site Scripting. **Upgrades available at:**	Beehive Forum SQL Injection or Cross-Site Scripting	High	Security Focus, 14361, 14363, July 25, 2005 **Security Focus,**

V0.6RC2	**http://prdownloads.sourceforge.net/beehiveforum/beehiveforum061.zip?do wnload** There is no exploit code required.			**14361, 14363, August 24, 2005**
QNX Software Systems Ltd. RTOS 6.3 .0, 6.1 .0	A vulnerability has been reported in the 'inputtrap' utility due to insufficient access control restrictions, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	QNX RTOS Information Disclosure CAN-2005-2725	Medium	Secunia Advisory: SA16569, August 25, 2005
ScriptsCenter Autolinks 2.1	A vulnerability has been reported in 'al_initialize.php' due to insufficient verification of the 'alpath' parameter before used to include files, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	AutoLinks Pro Include File Remote Arbitrary Code Execution	High	NewAngels Advisory #1, August 28, 2005
WebCalendar WebCalendar 1.0, RC1-RC3	A vulnerability has been reported in 'send_reminders.php' due to insufficient verification of the 'includedir' parameter, which could let remote malicious users execute arbitrary files. Upgrades available at: http://prdownloads.sourceforge.net/webcalendar/WebCalendar-1.0.1.tar.g z?download There is no exploit code required.	WebCalendar 'Send_Reminders.PHP' Remote Code Execution CAN-2005-2717	High	Security Focus, Bugtraq ID: 14651, August 24, 2005
YaPiG YaPig 0.95 b & prior	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of EXIF data stored in certain image files, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	YaPiG Cross-Site Scripting CAN-2005-2736	Medium	Security Tracker Alert ID: 1014802, August 26, 2005
Zaunz Publishing GmbH Cosmoshop 8.10 .78	Several vulnerabilities have been reported: an SQL injection vulnerability was reported due to insufficient sanitization of input passed in the administration login before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a vulnerability was reported in 'bestmail_edit.cgi' because the administration section can be accessed and sensitive information obtained via the 'file' parameter; and a vulnerability was reported because passwords are stored in clear text, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	Cosmoshop SQL Injection & Information Disclosure	Medium	Secunia Advisory: SA16625, August 30, 2005

[back to top]

Wireless

The section below contains wireless vulnerabilities, articles, and viruses/trojans identified during this reporting period.

- **Distance detection may help secure Wi-Fi:** A new way of locating a Wi-Fi user has been developed by Intel. It times how long it takes for packets to travel to and from a wireless access point, which could help prevent users outside a house or office from accessing a Wi-Fi network indoors. Source: http://www.networkworld.com/news/2005/082505-intel-wi-fi.html.
- **More U.S. Cities Pushing Public Wireless Nets:** In the past two years more than two dozen cities have built or are planning on building "metropolitan area networks" (MANs). Over the last few years Wi-Fi, technology has found an important place among digital consumers and access providers. An increasing number of U.S. cities are jumping on the bandwagon, ranging from large metropolitan areas to small rural townships. Source: http://abcnews.go.com/Technology/story?id=1048622&page=1.
- **Cell Phone 'Most Indispensable' Tool For Financial Execs:** According to a survey conducted by Robert Half Management Resources, cell phones remain the most indispensable tool for financial executives. About 44 percent of the 1400 chief financial officers (CFOs) participating in the survey. Source: http://www.informationweek.com/story/showArticle.jhtml;jsessionid=VEIHQ1C1EMQAAQSNDBGCKHSCJUMEKJVN?articleID=170100712.

Wireless Vulnerabilities

- WepDecrypt-0.7.tar.gz: A wireless LAN tool based on wepattack that guesses WEP keys using an active dictionary attack, a key generator, a distributed network attack, and some other methods.
- Nokia Affix BTSRV Device Name Remote Command Execution: An input validation vulnerability has been reported which could let a remote malicious user inject arbitrary shell commands. For more information see entry above.
- BlueZ Arbitrary Command Execution: A vulnerability has been reported due to insufficient sanitization of input passed as a remote device name, which could let a remote malicious user execute arbitrary code. Updated information regardin Mandriva patch.

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
August 30, 2005	hp_ovnnm_poc.c	Yes	Proof of Concept exploit for the HP OpenView Network Node Manager Remote Arbitrary Code Execution vulnerability.
August 29, 2005	bfccown.zip	No	Proof of Concept exploit for the BFCommand & Control Server Manager Multiple Remote Vulnerabilities.
August 29, 2005	looking_glass_poc lglass20040427.txt	No	Proofs of Concept exploit scripts for the Looking Glass Remote Command Execution vulnerability.
August 29, 2005	sphpblog_vulns.pl sphpblog.txt	No	Scripts that exploit the Simple PHP Blog Directory Traversal vulnerability.
August 29, 2005	xgopher-client.c	No	Exploit for the UMN Gopher Client Remote Buffer Overflow vulnerability.
August 28, 2005	aircrack-2.3.tgz	N/A	An 802.11 WEP cracking program that can recover a 40-bit or 104-bit WEP key once enough encrypted packets have been gathered.
August 28, 2005	GOT_Hijack.txt	N/A	A paper that discusses the method of overwriting a pointer used in a function for the sake of overwriting the associated entry in the Global Offset Table (GOT) which in turn allows for execution flow redirection.
August 28, 2005	proboscis.c	N/A	Proof of concept event interface keystroke logger that records everything coming through /dev/input/event*.
August 26, 2005	Evil.Shell.Backdoor_1.0.5.c	N/A	Password protected windows bind/reverse shell backdoor.
August 26, 2005	fileutils-4.1.txt	No	Proof of Concept exploit for the Fileutils Directory Trees Denial of Service vulnerability.
August 25, 2005	ThePharmingGuide.pdf	N/A	"The Phishing Guide", examines the name services of which Internet-based customers are dependent upon, and how they can be exploited by Pharmers to conduct identity theft and financial fraud on a massive scale.
August 24, 2005	bbcodeLogout.txt	No	Proof of Concept exploit for the BBCode vulnerability.
August 24, 2005	elmexPoC.c	Yes	Proof of Concept exploit for the Elm 'Expires' Header Remote Buffer Overflow vulnerability.
August 24, 2005	Mercora_IMRadio.c	No	Exploit script for the Mercora IMRadio Plaintext Password Disclosure vulnerability.
August 24, 2005	mybbSQLinject.txt file.pl	No	Proof of Concept exploits for the MyBB SQL Injection vulnerability.
August 24, 2005	netquery311.html	Yes	Proof of Concept exploit for the Netquery Input Validation vulnerability.
August 24, 2005	save_yourself_from_ savewebportal34.html	No	Exploitation details for the SaveWebPortal Multiple Vulnerabilities.
August 24, 2005	ventboom.zip	No	Exploit for the Ventrilo Status Requests Remote Denial of Service vulnerability.
August 24, 2005	WepDecrypt-0.7.tar.gz	N/A	A wireless LAN tool based on wepattack that guesses WEP keys using an active dictionary attack, a key generator, a distributed network attack, and some other methods.
August 24, 2005	WinAce2605.txt	No	Exploit for the WinAce Buffer Overflow vulnerability.
August 24, 2005	x_osh2-9byte.pl.txt	No	New version of an exploit for the Operator Shell (osh) 1.7-12 local root vulnerability.
August 24, 2005	ZipTorrent_poc.c	No	Proof of Concept exploit for the ZipTorrent Proxy Server Password Disclosure vulnerability.

[back to top]

Trends

- **Hidden-code flaw in Windows renews worries over stealthly malware:** A flaw in the way that several security programs and systems utilities detect system changes could allow spyware to spread surreptitiously. This has renewed worries about stealthier attack code. Source: http://www.securityfocus.com/news/11300.
- **Ten-Minute Guide To Network Security:** Security can be complex and an expensive and time-consuming business. Between upgrading LANs, putting out network fires, deploying new software, and making sure everything runs smoothly has many IT managers stretched to the limit. However, the security process can be started in ten minutes. Source: http://www.informationweek.com/story/showArticle.jhtml?articleID=170101541&tid=6004
- **The Threats Get Nastier:** According to InformationWeek Research's U.S. Information Security Survey 2005, conducted in July and August in partnership with management-consulting firm Accenture, IT professionals believe that the situation is under control when they were asked if their organizations were more vulnerable to malicious code attacks and security breaches than a year ago. Only 16% of survey participants say things have gotten worse. But the 'ready-for-anything' attitude can be misleading and even dangerous. Source: http://www.informationweek.com/story/showArticle.jhtml?articleID=170100709&tid=6004
- **Chinese Web sites used to target U.S. systems-report:** According to the Washington Post, web sites in China are being used as a staging ground for attacks on computer networks in the U.S. Defense Department and other agencies. No classified systems have been compromised but officials are concerned that data pulled together from different agencies could become useful intelligence to an adversary. Source: http://today.reuters.com/news/NewsArticle.aspx?type=internetNews&storyID=2005-08-25T051455Z_01_DIT518808_RTRIDST_0_NET-SECURITY

- **IM worm speaks your language:** Security experts are warning that a new MSN Messenger worm often talks to people in their own language. The worm, Kelvir.HI, tailors the language of its attack message to the compromised system. It can send messages in English, Dutch, French, German, Greek (English alphabet), Italian, Portuguese, Swedish, Spanish and Turkish. This is the first time that a worm checks the system settings and then sends a specific message. Source: http://news.com.com/IM+worm+speaks+your+language/2100-7349_3-5842767.html?tag=cd.lede.
- **Bots 'Dangerous' to Corporate Networks:** Bot attacks are becoming a critical security issue for IT and security administrators. Once the bot has circulated to other machines on the corporate network, a remote malicious user would have the ability to change company information, steal files, encrypt data or even shutting down the network. Source: http://www.esecurityplanet.com/trends/article.php/3529896.
- **Trojan Poses As Plug And Play Patch:** A new variant of the Downloader Trojan is circulating that presents to be a patch for the vulnerability outlined in the MS05-039 bulletin Microsoft released earlier in August. It is a new way of exploiting the Plug and Play vulnerability by using social engineering. Source: http://www.informationweek.com/story/showArticle.jhtml;jsessionid=VEIHQ1C1EMQAAQSNDBGCKHSCJUMEKJVN?articleID=170100880 .

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared files.
2	Mytob.C	Win32 Worm	Slight Increase	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
3	Zafi-D	Win32 Worm	Slight Decrease	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
4	Netsky-Q	Win32 Worm	Stable	March 2004	A mass-mailing worm that attempts to launch Denial of Service attacks against several web pages, deletes the entries belonging to several worms, and emits a sound through the internal speaker.
5	Mytob-BE	Win32 Worm	Slight Decrease	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.
6	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
7	Zafi-B	Win32 Worm	Increase	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
8	Netsky-D	Win32 Worm	Slight Increase	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
9	Netsky-Z	Win32 Worm	Decrease	April 2004	A mass-mailing worm that is very close to previous variants. The worm spreads in e-mails, but does not spread to local network and P2P and does not uninstall Bagle worm. The worm has a backdoor that listens on port 665.
10	Lovgate.w	Win32 Worm	Decrease	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.

Table updated August 27, 2005

[back to top]